IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPEAL TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN RE APPLICATION OF:	**BRUCE K. GEIST** **THOMAS D. HAYOSH**
EXAMINER:	**KAMBIZ ZAND**
APPLICATION NO.:	**09/707,433**
DOCKET NO.:	**PM021**
ART UNIT:	**2132**
FILED:	**NOVEMBER 7, 2000**
TITLE:	**SELF-AUTHENTICATION OF VALUE DOCUMENTS USING DIGITAL SIGNATURES**

TRANSMITTAL OF MAILING BY EXPRESS MAIL OF APPELLANTS' BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Commissioner for Patents
Mail Stop Appeal Brief - Patents
P. O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this Appellants' Brief To The Board of the Patent Appeals and Interferences in the above-identified application, along with any paper referred to as being attached or enclosed, is being deposited with United States Postal Service with sufficient postage as Express Mail on November 18, 2005 Express Mail Label No. EU455380091US.

The Commissioner for Patents is hereby authorized to charge payment of the required processing fee in the amount of $330.00 to Deposit Account No. 19-3790 as set forth in 37 C.F.R. 1.17(c). A duplicate of this sheet is attached.

Joseph P. C. Cifelli
(Print Name)

Joseph P. C. Cifelli
(Signature)

11-21-05

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN RE APPLICATION OF:

BRUCE K. GEIST
THOMAS D. HAYOSH

APPLICATION NO.: 09/707,433

FILED: NOVEMBER 7, 2000

TITLE: SELF-AUTHENTICATION OF VALUE DOCUMENTS USING DIGITAL SIGNATURES

EXAMINER: KAMBIZ ZAND

ART UNIT: 2132

APPELLANTS' BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Sir:

Appellant respectfully submits this Appellants' Brief, pursuant to 37 C.F.R. §1.192. It is filed within two (2) months from the filing of the Notice of Appeal on September 21, 2005 ("the Notice of Appeal"). All fees associated with the filing of this Appellants' Brief are also included herewith.

11/22/2005 DTESSEM1 00000047 193790 09707433
01 FC:1402 500.00 DA

CERTIFICATE OF MAILING (37 CFR 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail on November 18, 2005, in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Joseph P.C. Cifelli 11-18-05

(Joseph P.C. Cifelli) (Date)

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST:

UNISYS CORPORATION
ONE UNISYS WAY
BLUE BELL, PA 19424

Unisys Corporation is the real party in interest through an Assignment from all the inventors of their entire right, title, and interest, duly recorded on April 4, 2001 in the United States Patent and Trademark Office at Reel/Frame 011638/0565, said assignment comprising four (4) pages.

II. RELATED PENDING APPEALS AND INTERFERENCES:

There are no pending appeals or interferences related to this subject matter of this Appeal.

III. STATUS OF CLAIMS

The status of the claims in the subject application is as follows:

A. Summary of the Status of the Claims in the Application

The application was originally filed with claims 1-28. Concomitantly with the filing of the application, a preliminary amendment was filed in which claims 2-28 were canceled and claims 29-143 were added. Recognizing an inadvertent error in numbering, the Examiner renumbered claim numbers 136-143 to 137-144 in the first office action (*Office Action dated December 15, 2004*). Appellants canceled claim 1 thereafter in their Response dated May 16, 2005 (such claim having previously been kept for continuity purposes). At present, claims 29-144 stand rejected, and Appellants are appealing the rejection of these claims.

B. Status of all the Claims

1. Claims canceled: 1-28;
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims allowed: NONE
4. Claims rejected: 29-64, 72-85, 92-127, and 133-144;

5. Claims objected to: 65-71, 86-91 and 128-132;
6. Claims pending: 29-144; and,
7. Claims appealed: 29-144

Claims 29-144 are currently pending in the subject application and have been finally rejected in the Office Action dated July 21, 2005 (hereinafter "*Final Office Action*"). There are no other pending claims in the case.

More specifically, claims 1[a], 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 stand rejected under 35 U.S.C. §102(e) as being anticipated by United States Patent No. 6,289,323 B1 (Gordon et. al)(hereinafter, "Gordon"). Claims 38 and 52 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of United States Patent No. 5,337,358A (Axelrod et al.)(hereinafter, "Axelrod"). Claims 65-71, 86-91 and 128-132 are objected to as being dependent upon a rejected base claim, but were indicated as being allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims[b].

IV. STATUS OF THE AMENDMENTS

All amendments have been acted upon by the Examiner and entered prior to the filing of the Notice of Appeal. No other amendments are believed to be outstanding.

A clean set of claims 29-144 is provided in the Claims Appendix attached hereto.

[a] Appellants would note that, although the Examiner notes at page 2 of the Final Office Action that claim 1 was canceled, the §102 rejection is still applied as against this claim at page 4. Appellants submit that this is a typographical error, and as the rejection of claim 1 is moot, Appellants will not address same.

[b] Somewhat contrary to this finding of allowability at page 7 of the Final Office Action, the Examiner continues to object to the use of the term "critical document data." This objection was fully addressed in Appellants' Response to Final Office Action including Notice of Appeal, and such argument is incorporated by reference herein and attached hereto in the Evidence Appendix.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following summary is provided for each of the independent claims involved in the subject Appeal, such summary including exemplary references to the specification by page and line number, and to the drawings by reference characters. In addition, each means plus function and/or step plus function present in the independent claims (and those dependent claims argued separately) is also identified with exemplary reference to the specification by page and line number and to the drawings by reference characters.

Independent Claim 29 is directed to a self-authenticating document (e.g., check 45) having critical document data. (*See, e.g., page 15, lines 16-18 and pages 16-18, lines 6-34; 1-10; and figures 5 and 6 for discussion of critical document data*). The self-authenticating document includes a first digital signature having a first digest of the critical document data and a second digital signature including a second digest of the critical document data and a personal identification number (PIN) 43. (*See, e.g., pages 7-10 for general discussion of digital signatures and page 8, line 5 for "digest." See also, pages 17-18, lines 12-34; 1-6 for discussion of critical document data and personal identification number (PIN) 43. For additional support, see page 18, lines 8-22).* The self-authenticating document further includes a public key certificate 49 having an authentic public key for validating the first and second digital signatures (*See, e.g., pages 13-14, lines 1-34; 1-18 for general discussion of public key certificates. See also, page 23, lines 6-12; page 29, lines 6-13; page 37, lines 10-12).* The first digital signature, the second digital signature, and the public key certificate are stored on the self-authenticating document (*See, e.g., page 15, lines 16-18; page 29, lines 1-8; and figures 5 and 6 (fields 62, 65, 66)).*

Independent Claim 43 is also directed to a self-authenticating document (e.g., check 45) having critical document data. The digital signature including a digest of the critical document data and personal identification number (PIN) and a public key certificate including an authentic public key for validating the digital signature. The digital signature and the public key certificate are stored on the self-authenticating document. (*See, citations for claim 29, supra. See also generally at page 27, lines 6-34, and specifically, lines 15-16)*

Independent Claim 75 is drawn to a personal value document (e.g., check 45). The personal value document includes a first digital signature having a first digest of critical document data, where the

critical document data includes data contained in a magnetic ink character recognition (MICR) code line 90 on the personal value document. (*See, citations for claim 29, supra. See, also, e.g., page 16, lines 6-8; figure 5).* The personal value document further has a second digital signature including a second digest of the critical document data and a personal identification number (PIN) 43 and a public key certificate including an authentic public key for validating the first and second digital signatures. (*See, citations for claim 29, supra).* The first digital signature, the second digital signature, and the public key certificate are stored in a bar code format 60 on the personal value document. (*See, citations for claim 29, supra. See also, pages 29, lines 21-24 and figures 5 and 6*).

Independent Claim 93 is drawn to a self-authenticating document (e.g., check 45) having critical document data. The self-authenticating document includes a digital signature including a digest of the critical document data and a public key certificate including an authentic public key for validating the digital signature. The digital signature and the public key certificate are stored in machine-readable format on the self-authenticating document. (*See, citations for claim 29, supra. See also generally at pages 28-29, lines 1-34; 1-2)*

Independent Claim 100 is directed to a method for creating a self-authenticating document (e.g., check 45) having critical document data, the critical document data including machine-readable data printed on the self-authenticating document. (*See, e g., Figures 5 and 7*) A first digital signature is created by signing the critical document data with a digital signature algorithm (step 74) and a second digital signature is created by signing the critical document data critical document data and a personal identification number (PIN) 43 with the digital signature algorithm (Step 75). (*See, e.g., pages 32-33, lines 16-28; 1-2. See also, generally at pages 7-13 for discussion of digital signature algorithms and also pages 18-23. See, specifically at page 18, lines 8-22*). A public key certificate including an authentic public key for validating the first and second digital signatures is retrieved (step 76) (*page 33, lines 4-5*), and the first and second digital signatures and the public key certificate are affixed to the self-authenticating document in a machine-readable format (e.g., bar code 60 at step 80). (*See, e.g., page 29, lines 6-13)(See also, citations for claim 29, supra).*

Independent Claim 109 is drawn to a method for creating a self-authenticating document having critical document data, the critical document data including machine-readable data printed on the self-authenticating document (*See, e g., Figures 5 and 7a*) A first digital signature is created by signing the

critical document data with a digital signature algorithm (step 72a), a second digital signature is created by signing the critical document data and a personal identification number (PIN) with the digital signature algorithm (step 73a), and a public key certificate including an authentic public key for validating the first and second digital signatures is retrieved (step 76a). (*See, e.g., p. 34, lines 6-8. See also, citations for claim 100, supra*). Whether the first digital signature and/or the second digital signature is to be affixed to the self-authenticating document is determined (e.g., respectively at steps 78a and 81) (*See, e.g., page 34, lines 11-19).* The public key certificate and at least one of the first digital signature and the second digital signature is affixed to the self-authenticating document in machine-readable code, based on the results of the second digital signature and first digital signature determining steps (step 89a) (*See, e.g., page 35, lines 15-22 and page 29, lines 1-8*).

Independent Claim 119 is directed to a method of authenticating a self-authenticating document (*See, e.g., figure 9).* Machine-readable data (e.g., bar code data 60) on the self-authenticating document is processed to obtain digital signature data and a public key certificate (step 201)(*See, e.g., page 37, lines 22-30).* The public key certificate is processed to obtain public key certificate data including an authentic public key (step 203) and critical document data is assembled from the self-authenticating document (step 204), where the critical document data includes at least magnetic ink character recognition (MICR) data (e.g., MICR line 90) printed on the self-authenticating document. (*See, e.g., page 38, lines 5-13).* It is determined whether an authentic personal identification number (PIN) 43 is available for appending to the critical document data (step 205) and, if the authentic PIN is available, it is appended to the critical document data to create an authenticatable data string (step 207). (*See, e.g., page 38, lines 15-24*). The authentic public key is applied to the digital signature data to validate the authenticatable data string, and the self-authenticating document is authenticated if the authenticatable data string is validated (step 208) (*See, e.g., page 38, lines 22-27).*

Independent Claim 135 is directed to a system for reading a self-authenticating document having machine-readable data including critical document data, digital signature data and a public key certificate. (*See, e.g., figure 8*). The system (100) includes personal identification means (140) for receiving a personal identification number (PIN) from a presenter of the self-authenticating document and image scanning and processing means (110) for reading the self-authenticating document and retrieving the machine-readable data from the self-authenticating document, and for assembling an authenticatable data string from the critical document data and the received PIN 43. (*See, e.g., page 36,*

lines 15-23) The system further includes parsing means (120) for parsing the machine readable data to obtain the digital signature data and the public key certificate and, validating means (130) for certifying the public key certificate to obtain an authentic public key, and for applying the authentic public key to the digital signature data for validating the authenticatable data string, wherein the self-authenticating document is authenticated if the authenticatable data string is validated. (*See, e.g., pages 36-37, lines 23-34; 1-8*)

Independent Claim 140 is directed to a system for reading a self-authenticating document, having machine-readable data including first critical document data stored on a magnetic ink character recognition (MICR) line, and first and second digital signatures, and a public key certificate stored on a bar code line. *(See, e.g., figures 5, 6, 8, and 9*). The system a personal identification subsystem (140) for receiving a personal identification number (PIN) 43 from a presenter of the self-authenticating document, and an image scanner and processor system (110) for reading the self-authenticating document, retrieving the machine readable data from the self-authenticating document, and for assembling an authenticatable data string from the first critical document data and the received PIN 43. (*See, e.g., page 36, lines 15-23*). The image scanner and processor system (110) includes: a magnetic ink character recognition (MICR) reader subsystem (112) for retrieving the first critical document data from the MICR line 60 and a bar code reader subsystem (114) for retrieving the first and second digital signatures and the public key certificate stored on a bar code line 60 (*Id. at lines 20-24*). The image scanner and processor system (110) further includes a parsing subsystem (120) for parsing the bar code 60 to obtain the first and second digital signatures and the public key certificate and a validating subsystem (130) for certifying the public key certificate to obtain an authentic public key and for applying the authentic public key to at least the second digital signature for validating the authenticatable data string. (*See, e.g., pages 36-37, lines 24-28; 1-14*). The self-authenticating document is authenticated if the authenticatable data string is validated. (*Id. See also, page 38 at lines 25-26; page 40, lines 1-5).*

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. **Claims 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gordon**

B. **Claims 38 and 52 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of Axelrod**

VII. ARGUMENT

A. Claims 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gordon

Claims 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gordon. Appellants respectfully traverse this rejection for at least the reasons set forth below.

Gordon discloses a method and apparatus for secure goods and services transactions via the postal service using an authenticated payment scheme. In the disclosed embodiment, a person or entity having an account with a postal authority issues a value message 14 in exchange for goods or services through a Payer Postal Security Device (PSD) 12. (*Gordon,* Col. 3, lines 12-15). The merchant exchanging the goods or services for the value message endorses the message with another PSD 16, and the endorsed value message 17 is then presented to the postal authority 10 for authentication. (*Id.*, lines 17-21). If the message is authenticated, the Payer PSD 12 is debited, and the payee PSD 16 is credited. (*See, id.* lines 22-24).

The value message 14 includes both text fields and encoded graphics such as one- or two-dimensional barcodes. The text fields include an algorithm ID 32, which identifies the type of cryptographic transformation algorithm used to render the Payer digital signature 50, a PSD certificate serial number 34, a Payee ID 46, and a Payer digital signature 50. (*Id at* Figure 2 and Cols. 6-7). PSD certificate serial number 34 identifies the serial number for that certificate used to authenticate the public/private key combination issued to the Payer PSD 12 by a Certificate Authority. It enables the postal authority 10 to select from a public key database, the public key that corresponds to the private key used by the Payer PSD 12 to create the digital signature 50 for the value message 14. (Thus, the Payer PSD 12 need not include the public key with the value message 14.) (*Id.*, Col 6, lines 45-51). Payer

digital signature 50 is a hashed, cryptographically transformed representation of all the data fields in value message 14. (*Id.*, Col 8, lines 6-10). The Payer PSD 12 digitally signs these data fields using Payer's private key based on public/private key cryptography. (*Id. at* Col. 4, lines 24-40).

Once a payer issues the value message 14 to the merchant, the merchant endorses the value message 14 using a Payee PSD 16, which results in an endorsed value message 17. During the endorsement process the merchant adds additional data and fields, including an algorithm ID 52, provided in barcode form only, to identify the type of cryptographic algorithm used to render the Payee digital signature and a Payee digital signature 54 (discussed below) which is also rendered in graphical barcode format on the endorsed value message 17. (*Id.*, lines 55-60).

The Payee digital signature 54 is based upon all of the data fields contained in the endorsed value message 17. As with the Payer digital signature 50, Payee digital signature 54 is also based on public/private key cryptography, but Payee digital signature 54 uses the Payee's private key. (*Id.*, lines 44-52; Col 8, lines 29-32).

1. Claims 29-118 - Gordon Does Not Teach or Suggest Appellants' Claimed Invention wherein the Public Key Certificate, Including Public Key, is Stored on the Document and, in fact, Teaches Away from Such Limitation

Independent claims 29, 43, 75, 93, 100 and 109 set forth, in pertinent part, that the public key certificate including an authentic public key that will be used for validating the digital signature contained on the self-authenticating document is itself stored on the self-authenticating document. Gordon neither teaches nor suggests storing the public key certificate (and thus public key) on the document, in fact, teaches away from this limitation.

It is well-accepted law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. (*See,* Manual of Patent Examination Procedure (MPEP) §2131, *citing* *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). Thus, if any element is missing, a finding of anticipation under §102 cannot stand.

As set forth above, the public key of both Payer and Payee in Gordon's invention is obtained via a public "keyring." More specifically, as stated above, Gordon teaches that the postal authority 10 selects a public key from a public key database maintained by the postal authority 10. Thus, with regard to the Payer device (PSD 12):

> *A PSD certificate serial number 34, provided in barcode form only, identifies the serial number for the certificate used to authenticate the public/private key combination issued to the Payer PSD 12 by a Certificate Authority.* ***The PSD certificate serial number 34 enables the postal authority 10 to select a public key from a public key database maintained by the postal authority 10.*** *The public key corresponds to a private key used by the Payer PSD 12 to create a digital signature for the value message 14.* ***Thus, the Payer PSD 12 need not include the public key with the value message 14.***

[*Gordon*, Col. 6, lines 45-54](Emphasis added). And, with regard to the Payee device (PSD 16):

> *The endorsed value message 17 includes a set of additional fields for authentication and record keeping. An algorithm ID 52, provided in barcode form only, identifies the type of cryptographic transformation used to render a payee digital signature 54 appended by the Payee PSD 16 when the endorsed value message 17 is issued by the Payee PSD 16.* ***The payee digital signature 54 is cryptographically transformed by means of a public key stored at the postal authority 10 and accessed based upon the payee identification 46.*** *Finally, the endorsed value message 17 includes a date/time 56 which specifies when the Payee PSD 16 issued the endorsed value message 17.*

[Id., Col. 8, lines 29-34](Emphasis added).

For this reason alone, claims 29, 43, 75, 93, 100 and 109 are not anticipated by Gordon, and are therefore patentable thereover. As claims 30-42, 44-74, 76-92, 94-99, 101-108, and 110-118 are dependent directly or indirectly from these claims, they too are patentable over Gordon.

However, not only does Gordon not teach this limitation, but it also teaches away from Appellants' invention of storing the public key certificate, including the authentic public key, on the self-authenticating document, for it clearly states (as shown in the bolded section, *supra*) that by allowing the public key to be stored in a public key database maintained by the postal authority, "*the Payer PSD 12 need not include the public key with the value message 14.*" (*Id.*, Col. 6, lines 53-54).

The Examiner sets forth in the Final Office Action that this argument cannot stand because Gordon's statement that the public key certificate "need not include the public key with the value message" merely means that "*such inclusion is not necessary, and that [it] is an option and not the only solution.*" (Final Office Action, p. 4). The Examiner's response is flawed for at least the fact that, in

responding to Appellants' arguments regarding this missing limitation, he fails to address those arguments made against the 35 U.S.C. §102(e) rejection, and merely responds to Appellants' arguments against an anticipated obviousness rejection. That is, the Examiner fails to address the initial point raised by Appellants that Gordon does not anticipate Appellants' claimed invention under 35 U.S.C. §102(e) because all limitations of the relevant claims are not disclosed.

Additionally, while Appellants admit that the phrase "*need not*" may be understood in common English usage to mean "not required" or "not necessary," when taken in the abstract, a careful review of the context in which this phrase is given in Gordon (and in light of the invention itself) reveals that a better interpretation would be that Gordon is stating that as a direct benefit of his invention, the public keys can be stored outside of the message on public keyrings/databases, thus specifically ***avoiding*** the need to include them on the value message 14. Under such interpretation, one skilled in the art would not look to Gordon for teaching Appellants' claimed invention of a self-authenticating document which, in part, depends on affixing the public key certificate and public key to the value document. Thus, Gordon clearly teaches away from Appellants' claimed invention, and the Examiner's arguments cannot stand.

For these additional reasons, claims 29-118 are not anticipated by Gordon under 35 U.S.C §102(e), and are therefore patentable thereover.

2. Claims 29-42, 75-92, and 100-118 – Gordon Neither Teaches nor Suggests Appellants' Claimed Invention wherein the Same Public/Private Key Pair is Used To Create the First and Second Digital Signature and, in fact, Teaches Away from Such Limitation

In addition to the reasons set forth above, claims 29-42, 75-92, and 100-118 are also patentable over Gordon for the reason that Gordon does not teach or suggest that the same public/private key pair is used to create the first and second digital signature.

Independent claims 29, 75, 100 and 109 set forth, in pertinent part, that the authentic public key included in the authentic public key certificate is used to validate both the first and second digital signatures contained in the self-authenticating document. Conversely, as discussed above, Gordon's invention necessitates that distinct and separate public/private key pairs be used; one for the Payer (in order to create Payer digital signature 50), and another for the Payee (in order to create Payee digital signature 54). In addition, Gordon teaches away from Appellants' invention because, given the purpose

of the two digital signatures in Gordon – ability to authenticate distinct parties- i.e., Payer and Payee – one would not look to Gordon for the teaching of applying the same public/private key pair.

The Examiner maintains that the identical nature of the public/private key pair is not recited in the subject claims, and may not be read into the claim from the specification (Final Office Action, p. 3). The Examiner's argument is in error for at least the following reason:

As set forth in the subject application, and as will also be appreciated from the well-known principles of public/private key cryptography, public and private keys in a public/private key cryptographic system are related in such a way that:

> *only the public key which is companion to the private key used to produce the digital signature will successfully verify the message/digital signature combination*

(*09/707,433 Application*, p. 10, lines 11-14). Therefore, that the same public key is used to validate both the first and second digital signatures ***necessitates*** that the same private key be used to create them.

Independent claims 29, 75, 100 and 109 clearly set forth that the authentic public key is used to validate both the first and second digital signatures contained in the self-authenticating document. Based on the foregoing principles and arguments, it must be inferred then that the same private key is used to create both the first and second digital signatures. Therefore, as both the first and second digital signatures have the same private and public key, the public/private key pairs may be said to be identical, and the Examiner's argument cannot stand.

For the additional reason set forth in this subheading, claims 29, 75, 100 and 109 are not anticipated by Gordon under 35 U.S.C. §102(e), and are therefore patentable thereover. As claims 30-42, 76-92, 101-108, and 110-118 are dependent directly or indirectly from these claims, they too are patentable over Gordon.

3. **Claims 40-42, 54-55, 79-80, 99** - Gordon Fails to Teach or Suggest Appellants' Claimed Invention wherein the Bar Code has a Plurality of Data Fields Including a Data Field for Representing the Number of Bytes of Data in a Bar Code and a Data Field for Representing the Number of Bytes of Data in the Critical Document Data

In addition to the reasons set forth in the foregoing subheadings, claims 40-42, 54-55, 79-80, 99 are patentable over Gordon under 35 U.S.C. §102(e) because Gordon does not teach or suggest Appellants' claimed invention wherein the bar code has a plurality of data fields including a data field for representing the number of bytes of data, ***k***, in a bar code (61) and a data field for representing the number of bytes of data, ***l***, in the critical document data (63) (*See, Id. at Figure 6*). As set forth in greater detail at pages 40-42 of Appellants' application (*see Evidence Appendix*), in a preferred embodiment of the Appellants' invention, these fields are necessary for determining whether the first and/or second digital signature is present on the self-authentication document during the authentication of same.

As seen with reference to Figure 2 of Gordon in conjunction with the relevant portions of the specification (*see, Cols. 6-8*), although Gordon teaches in great detail a value message comprising a plurality of fields, there is no teaching or suggestion of these particular data fields. The Examiner does not point to such teaching in support in his rejection of these claims, merely stating that Gordon "*disclose[s] a barcode format include[ing] a number of fields as recited in the...claims.*"(*Final Office Action*, p.6). However, this is insufficient support for a rejection under 35 U.S.C. §102, and for this reason alone, the rejection of these claims cannot stand.

Furthermore, Appellants submit that there is no need for these data fields in Gordon. As the value message of Gordon requires both the Payer digital signature 50 and payee digital signature 54 must be present for his system to be operable, there need be no determination as to whether one or the other digital signatures is present on the value message. Since the determination is unnecessary, data fields representing the number of bytes of data in the bar code and the number of bytes of data in the critical document data are unnecessary.

It will therefore be appreciated that for the additional reason set forth in this subheading, dependent claims 40-42, 54-55, 79-80, 99 are not anticipated by Gordon under 35 U.S.C. §102(e), and are therefore patentable thereover.

4. Claims 109-118 - Gordon Does Not Teach or Suggest Determining whether the First and Second Digital Signatures are to be Affixed to the Self-Authenticating Document and, in fact, Teaches Away from Such Limitation

In addition to the reasons regarding patentability over Gordon set forth in the foregoing subheadings, claims 109-118 are patentable over Gordon for the following reason. Independent claim 109 sets forth the steps of determining whether the second digital signature is to be affixed to the self-authenticating document, determining whether the first digital signature is to be affixed to the self-authenticating document, and then affixing the public key certificate and at least one of the first digital signature and the second digital signature to the self-authenticating document in machine-readable code, based on the results of the second digital signature and first digital signature determining steps. Nowhere does Gordon teach or suggest this and, in fact, Appellants submit that Gordon teaches away from these limitations for, in order for the system of Gordon to be operable, both the Payee and Payer digital signatures (54,50) must be present on the value message 17.

Thus, for the additional reason set forth in this subheading, independent claim 109 is not anticipated by Gordon under 35 U.S.C. §102(e), and is therefore patentable thereover. As claims 110-118 are dependent directly or indirectly from this claim, they too are patentable over Gordon.

5. Claims 119-120 - Gordon Neither Teaches nor Suggests Determining Whether an Authentic Personal Identification Number (PIN) is Available for Appending to the Critical Document Data

Independent claims 119 sets forth a method for authenticating a self-authenticating document. In relevant part, the method includes the steps of determining whether an authentic personal identification number (PIN) is available for appending to the critical document data. If the authentic PIN is available, it is appended to the critical document data to create an authenticatable data string and then the authentic public key is applied to the digital signature data to validate the authenticatable data string. The self-authenticating document is authenticated if the authenticatable data string is validated.

The Examiner does not point out where in Gordon these claimed limitations, and Appellants submit that Gordon fails to teach or suggest same. In fact, Appellants note that Gordon *requires* that the user enter a PIN in order to gain access to the Payer PSD 12:

> *The steps for vending, endorsing and negotiating the value message defined in FIG. 2 are summarized in FIG. 4. At step 200 the vending stage begins with a*

> *user entering a payer identification and/or PIN on the Payer PSD 12. The PIN is a private access number that must be entered for the identified payer identification in order to gain access to the value message issuing functionality of the Payer PSD 12.*

(*Gordon,* Col. 9, lines 24-27). Therefore, Appellants submit that not only does Gordon not teach this claimed feature, but he teaches away from it.

Thus, for the added reason set forth in this subheading, independent claims 119 is not anticipated by Gordon under 35 U.S.C. §102(e), and is therefore patentable thereover. As claims 120 is dependent directly or indirectly from this claim, it too is patentable over Gordon.

6. Claims 121-134 - Gordon Does Not Teach or Suggest Appellants' Claimed Invention of Determining whether a First Digital Signature is Present in the Digital Signature Data, if it is Determined that the Authentic Personal Identification Number (PIN) is not Available.

Claims 121-134 depend directly or indirectly from claim 119 and thus are patentable for the reasons set forth, *supra*. These claims are additionally patentable over Gordon for the reason that Gordon does not teach or suggest at least the additional steps set forth in claim 121; namely, if it is determined that the authentic personal identification number (PIN) is not available (such as in backroom operations where the customer is not available), determining whether a first digital signature is present in the digital signature data and applying the authentic public key to the digital signature data to validate the critical document data, wherein the self-authenticating document is authenticated if the critical document data is validated.

Again, Gordon requires that the user enter a PIN in order to gain access to the Payer PSD 12. If the PIN is not available (or is erroneous), an error message will be provided:

> *The PIN is a private access number that must be entered for the identified payer identification in order to gain access to the value message issuing functionality of the Payer PSD 12. In response, the Payer PSD 12, at step 202, compares the entered payer identification and PIN to a corresponding data entry in the Payer PSD 12 If the values do not match, then control passes to step 204 where the Payer PSD 12 issues an error indication, increments an error counter (if an incorrect PIN was entered for a valid payer identification, and the Payer PSD 12 compares the number of consecutive PIN entry errors to a prescribed limit.*

(*Id at* Col. 9, lines 26-38). It is irrelevant whether the Payer digital signature 50 and/or the Payee digital signature 54 is present.

For this additional reason, dependent claim 121 is not anticipated by Gordon, and is therefore patentable thereover. As claims 122-134 are dependent directly or indirectly from this claim, they too are patentable over Gordon.

7. Claims 122 and 123 – Gordon Fails to Teach or Suggest Determining whether a Second Digital Signature is Present in the Digital Signature Data and, if the Second Digital Signature is Present, Generating a Plurality of PINS, Appending each of the Plurality of PINS to the Critical Document Data to Create a Plurality of Verifiable Data Strings.

Claim 122 and 123, respectively dependent directly and indirectly from claim 121, are patentable over Gordon for all of the reasons set forth in the foregoing subheadings. In addition, these claims are patentable over Gordon because Gordon does not disclose or suggest the limitation that where if it is determined that both the authentic PIN is not available and the first digital signature is not present in the digital signature data, then it is determined whether a second digital signature is present in the digital signature data, and, if the second digital signature is present, a plurality of PINs is generated and then each of the plurality of PINs is appended to the critical document data to create a plurality of verifiable data strings. The authentic public key is then applied to the second digital signature in order to validate one of the verifiable data strings as the authenticatable data string and to authenticate the self-authenticating document.

Again, as set forth with respect to claims 121 and 124-134, Gordon requires a PIN in order for a user to gain access to the PSD 12: it is irrelevant whether the Payer digital signature 50 and/or the Payee digital signature 54 is present. While Gordon teaches allowing repeated attempts of a PIN by a user up to a prescribed limit (*see cite, supra*), unlike Appellants' claimed invention, these repeated attempts are not a plurality of PINs generated to append to critical document data in order to create verifiable data strings that are later compared as against the decrypted second digital signature.

Therefore, for this additional reason, dependent claims 122 and 123 are not anticipated by Gordon, and are patentable thereover.

8. Claims 135-144 - Gordon Does Not Teach or Suggest Several Elements of Appellants' Claimed Systems of Reading a Self-Authenticating Document

Independent claims 135 and 140 are similar claims drawn to a system for reading a self-authenticating document. Gordon does not teach or suggest at least several elements of both these claims.

Appellants' claimed invention includes personal identification means (subsystem in claim 140) "*for receiving a personal identification number (PIN) from a presenter of said self-authenticating document.*" The Examiner cites Gordon, Col. 4, lines 18-21 for teaching this limitation (*Final Office Action,* p. 5). This section sets forth the following:

> *The text fields include a payer identification, a payee identification, a value assigned the value message by the payee, and a time/date that the value message was issued by the payee. The text fields will be described herein below in conjunction with a description of FIG. 2.*

Thus it appears to be the Examiner's contention that the Payer and Payee identification fields are equivalent to Appellants' PIN. However, as they are both part of value message 14 issued by the payer PSD 12, they therefore cannot be received from a presenter of self-authenticating document. For this reason, Gordon does not teach this limitation.[c]

Claims 135 and 140 also set forth image scanning and processing means (subsystem in claim 140) "*for reading said self-authenticating document and retrieving said machine-readable data from said self-authenticating document, and for assembling an authenticatable data string from said critical document data and said received PIN.*" Again, unlike Appellants' claimed invention, the Payer and Payee identification fields identified by the Examiner as being equivalent to Appellants' PIN are not assembled with other critical document data to form an "authenticatable data string." Instead they are merely used to identify Payer and Payee. In fact, even were one to assert that the access PIN for Payer PSD 12 were equivalent to Appellants' PIN (an assertion not put forth by the Examiner), Gordon still would not teach this limitation because, as seen in the citation of subheading 6 *supra*, the user PIN in Gordon is merely for valid payer identification: it is not used for assembling an authenticatable data string.

In addition to the above missing elements, Gordon also does not teach or suggest parsing means (subsystem in claim 140) that parse "*machine readable data to obtain said digital signature data and said public key certificate,*" or validating means (subsystem in claim 140) "*for certifying said public key certificate to obtain an authentic public key*" because, again, neither the public key certificate nor the authentic public key is stored on Gordon's value message 17 (or 14).

[c] Appellants note that the Examiner does not assert that the PIN used to gain access to the Payer PSD 12, as discussed in the foregoing subheadings, is equivalent to that of Appellants' PIN.

For the reasons set forth herein, independent claims 135 and 140 are not anticipated by Gordon, and are therefore patentable thereover. As claims 136-139 and 141-144 are dependent directly or indirectly from these claims, they too are patentable over Gordon.

B. Claims 38 and 52 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of Axelrod.

Claims 38 and 52, respectively indirectly dependent from claims 29 and 43, stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of Axelrod. Each of these claims sets forth that the bar code format is PDF 417.

Although not dispositive before the Board, the United States Patent and Trademark Office's Manual of Patent Examining Procedures sets forth three basic criteria that must be met in order to establish a *prima facie* case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. (*M.P.E.P §2143*). Further, the teaching or suggestion to make the claimed combination must not use impermissible hindsight and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. (*Id., citing In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Axelrod teaches an apparatus for recording a transaction involving the authentication of an identification card. The identification card contains information pertaining to an object or other entity to be identified on a first portion of the card in human recognizable form, and a coded representation of an encrypted signal comprising a representation of the information on a second portion of the card. (*Axelrod*, Abstract).

Gordon does not teach or suggest several of the limitations of the independent claims from which these claims depend, and Axelrod does not does not provide the missing teaching. In fact, as set forth above, the Examiner merely cites Axelrod for teaching a PDF 417 bar code format in a transaction including authentication of an identification card. As the combination of Gordon and Axelrod does not teach or suggest all of the claim limitations of claims 38 and 52, the Examiner has not established a *prima facie* case of obviousness, and his rejection of these claims under 35 U.S.C. 103(a) cannot stand.

For the additional reasons set forth herein, dependent claims 38 and 52 are patentable over Gordon in view of Axelrod.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For all of the reasons set forth herein, the Examiner has failed to make a *prima facie* case under 35 U.S.C. §102(b) and 35 U.S.C. §103(a), and Appellant's application is patentable over the Gordon and Axelrod references. Appellant therefore comes before this Board and respectfully requests that the rejections be overturned, the claims be allowed, and the application pass to issuance.

Respectfully submitted,
BRUCE K. GEIST
THOMAS D. HAYOSH

BY: _____

LISE A. RODE
ATTORNEY FOR APPELLANT
REG. NO. 37,226

UNISYS CORPORATION
ONE UNISYS WAY
M/S E8-114
BLUE BELL, PENNSYLVANIA 19424
(215) 986-5169

IX. CLAIMS APPENDIX

29. A self-authenticating document having critical document data, comprising:

a first digital signature including a first digest of said critical document data;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored on said self-authenticating document.

30. The self-authenticating document of claim 29, wherein said first digital signature, said second digital signature, and said public key certificate are stored in machine-readable format on said self-authenticating document.

31. The self-authenticating document of claim 30, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

32. The self-authenticating document of claim 31, wherein said critical document data further includes ASCII text from said document.

33. The self-authenticating document of claim 32, wherein said ASCII text is the account name and address printed on said self-authenticating document.

34. The self-authenticating document of claim 31, wherein said document is a personal value document.

35. The self-authenticating document of claim 34, wherein said personal value document is a personal check.

36. The self-authenticating document of claim 34, wherein said personal value document is selected from the group consisting of: an identification card, a Social Security card, a driver's license, a birth certificate, a credit card, a voter's registration card, and a passport.

37. The self-authenticating document of claim 30, wherein said machine-readable format is a bar code.

38. The self-authenticating document of claim 37, wherein said bar code format is PDF 417.

39. The self-authenticating document of claim 37, wherein said bar code comprises a plurality of data fields.

40. The self-authenticating document of claim 39, wherein said bar code includes:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

41. The self-authenticating document of claim 40, wherein said bar code further includes a fifth data field including said second digital signature.

42. The self-authenticating document of claim 40, wherein said bar code further includes a sixth data field including said first digital signature.

43. A self-authenticating document having critical document data, comprising:

a digital signature including a digest of said critical document data and personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said digital signature, wherein said digital signature and said public key certificate are stored on said self-authenticating document.

44. The self-authenticating document of claim 43, wherein said digital signature and said public key certificate are stored in machine-readable format on said self-authenticating document.

45. The self-authenticating document of claim 44, wherein said document is a personal value document.

46. The self-authenticating document of claim 45, wherein said personal value document is a personal check.

47. The self-authenticating document of claim 45, wherein said personal value document is selected from the group consisting of: an identification card, a Social Security card, a driver's license, a birth certificate, a credit card, a voter's registration card, and a passport.

48. The self-authenticating document of claim 45, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

49. The self-authenticating document of claim 48, wherein said critical document data further includes ASCII text from said self-authenticating document.

50. The self-authenticating document of claim 49, wherein said ASCII text is the account name and address printed on said self-authenticating document.

51. The self-authenticating document of claim 44, wherein said machine-readable format is a two-dimensional bar code.

52. The self-authenticating document of claim 51, wherein said two-dimensional bar code format is PDF 417.

53. The self-authenticating document of claim 51, wherein said two-dimensional bar code comprises a plurality of two-byte data fields.

54. The self-authenticating document of claim 53, wherein said two-dimensional bar code includes:
a first data field including data representing the number of bytes of data in said bar code;
a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

55. The self-authenticating document of claim 54, wherein said two-dimensional bar code further includes a fifth data field including said digital signature.

56. The self-authenticating document of claim 43, wherein said personal identification number is a four digit number comprising four bytes of data.

57. The self-authenticating document of claim 43, wherein said personal identification number is selected by the owner of said personal value document.

58. The self-authenticating document of claim 43, wherein a third party responsible for printing said personal value document selects said personal identification number.

59. The self-authenticating document of claim 43, wherein a third party responsible for issuing said personal value document selects said personal identification number.

60. The self-authenticating document of claim 43, wherein the digital signature algorithm used to create said digest of said digital signature is a public key cryptographic algorithm.

61. The self-authenticating document of claim 60, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

62. The self-authenticating document of claim 43, wherein said public key certificate further includes identity information of the owner of said authentic public key and a digital signature of said authentic public key and said owner identity information, and wherein said digital signature is issued by a third party.

63. The self-authenticating document of claim 62, wherein said third-party digital signature is created using the elliptic curve digital signature algorithm (ECDSA).

64. The self-authenticating document of claim 63, wherein said ECDSA algorithm includes a first group of shared parameters for implementing said digital signature.

65. The self-authenticating document of claim 64, wherein said ECDSA used to create said third-party digital signature includes a second group of shared parameters for implementing said third-party digital signature.

66. The self-authenticating document of claim 65, wherein said first group of shared parameters is the same as said second group of shared parameters.

67. The self-authenticating document of claim 65, wherein said first group of shared parameters is different from said second group of shared parameters.

68. The self-authenticating document of claim 65, wherein said first and second groups of shared parameters is distributed to a community of users of said self-authenticating document.

69. The self-authenticating document of claim 68, wherein said third party is a certificate authority.

70. The self-authenticating document of claim 68, wherein said community of users includes a party responsible for issuing said self-authenticating document, a party responsible for printing said self-authenticating document, and said certificate authority.

71. The self-authenticating document of claim 70, wherein said community of users further includes an owner of said self-authenticating document.

72. The self-authenticating document of claim 43, wherein said public key certificate is affixed to said self-authenticating document by a third party responsible for printing said self-authenticating document.

73. The self-authenticating document of claim 43, wherein said public key certificate is affixed to said self-authenticating document by a third party responsible for issuing said public key certificate.

74. The self-authenticating document of claim 73, wherein said third party is a certificate authority.

75. A personal value document, comprising:

a first digital signature including a first digest of critical document data, said critical document data including data contained in a magnetic ink character recognition (MICR) code line on said personal value document;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored in a bar code format on said personal value document.

76. The personal value document of claim 75, wherein said personal value document is a personal check.

77. The personal value document of claim 75, wherein said critical document data further includes ASCII text from said personal check.

78. The personal value document of claim 77, wherein said ASCII text is the account name and address printed on said personal check.

79. The personal value document of claim 77, wherein said bar code comprises a plurality of date fields, including:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

80. The personal value document of claim 79, wherein said two-dimensional bar code further includes:

a fifth data field including said second digital signature; and,

a sixth data field including said first digital signature.

81. The personal value document of claim 75, wherein the digital signature algorithm used to create said first digest of said first digital signature and said second digest of said second digital signature is a public key cryptographic algorithm.

82. The personal value document of claim 81, wherein the digital signature algorithm used to create said first digest is the elliptic curve digital signature algorithm (ECDSA).

83. The personal value document of claim 82, wherein the digital signature algorithm used to create said second digest is the elliptic curve digital signature algorithm (ECDSA).

84. The personal value document of claim 75, wherein said personal identification number is selected by the owner of said personal value document.

85. The personal value document of claim 83, wherein said public key certificate further includes identity information of the owner of said authentic public key and a digital signature of said authentic public key and said owner identity information, and wherein said digital signature is issued by a certificate authority.

86. The personal value document of claim 85, wherein said ECDSA used to create said first and second digital signatures respectively includes a first group of shared parameters for implementing said first and second digital signatures, and wherein said ECDSA used to create said certificate authority digital signature includes a second group of shared parameters for implementing said certificate authority digital signature.

87. The personal value document of claim 86, wherein said first group of shared parameters is the same as said second group of shared parameters.

88. The personal value document of claim 86, wherein said first group of shared parameters is different from said second group of shared parameters.

89. The personal value document of claim 86, wherein said first and second groups of shared parameters is distributed to a community of users of said personal value document.

90. The personal value document of claim 89, wherein said community of users includes a party responsible for issuing said personal value document, a party responsible for printing said personal value document, and said certificate authority.

91. The personal value document of claim 90, wherein said community of users further includes an owner of said personal value document.

92. The personal value document of claim 75, wherein said first and second digital signatures, and said public key certificate are affixed to said personal value document by a third party responsible for printing said personal value document.

93. A self-authenticating document having critical document data, comprising:

a digital signature including a digest of said critical document data; and,

a public key certificate including an authentic public key for validating said digital signature, wherein said digital signature and said public key certificate are stored in machine-readable format on said self-authenticating document.

94. The self-authenticating document of claim 93, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

95. The self-authenticating document of claim 94, wherein said critical document data further includes ASCII text from said self-authenticating document.

96. The self-authenticating document of claim 94, wherein said self-authenticating document is a commercial value document.

97. The self-authenticating document of claim 96, wherein said commercial value document is selected from the group consisting of: a bank check, a business check, tickets, gift certificates, titles, negotiable letters of credit, and currency.

98. The self-authenticating document of claim 96, wherein said machine-readable format is a bar code, said bar code comprising a plurality of data fields.

99. The self-authenticating document of claim 98, wherein said code includes:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data;

a fourth data field including said critical document data; and,

a fifth data field including said digital signature.

100. A method for creating a self-authenticating document having critical document data, said critical document data including machine-readable data printed on said self-authenticating document, said method comprising the steps of:

creating a first digital signature by signing said critical document data with a digital signature algorithm;

creating a second digital signature by signing said critical document data critical document data and a personal identification number (PIN) with said digital signature algorithm;

retrieving a public key certificate including an authentic public key for validating said first and second digital signatures; and,

affixing said first and second digital signatures and said public key certificate to said self-authenticating document in a machine-readable format.

101. The method of claim 100, wherein said critical document data includes ASCII text from said self-authenticating document, and further comprising the step of:

storing said ASCII text in a machine-readable format on said self-authenticating document prior to said first digital signature creating step.

102. The method of claim 100, further comprising the steps of:

selecting a group of shared parameters corresponding to said digital signature algorithm for implementing said first and second digital signatures;

generating a public key and a private key using said shared parameters;

certifying said public key via a certificate authority,

wherein said selecting, generating and certifying steps are carried out prior to said first digital signature creation step.

103. The method of claim 100, wherein said step of creating said first digital signature includes the substeps of:

generating a public key and a private key using said digital signature algorithm;

assembling said critical document data from said self-authenticating document; and,

applying said private key generated by said digital signature algorithm to said critical document data to create said first digital signature.

104. The method of claim 103, wherein said step of creating said second digital signature includes the substeps of:

generating said personal identification number (PIN);

appending said personal identification number (PIN) to said critical document data to create an authenticatable data string; and,

applying said private key generated by said digital signature algorithm to said authenticatable data string to create said second digital signature.

105. The method of claim 104, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

106. The method of claim 104, wherein said step of affixing said first and second digital signatures to said self-authenticating document includes the substeps of:

assembling a k – byte data string, wherein k includes the number of bytes in said critical document data, said authenticatable data, and said public key certificate; and,

generating a machine-readable data string from said k – byte data string.

107. The method of claim 106, further comprising the step of calculating the total amount of bytes of data, k , including said critical document data, said authenticatable data string, and said public key certificate, prior to said k – byte data string assembling step.

108. The method of claim 107, wherein said first and second digital signatures and said public key certificate are affixed in bar-code format to said self-authenticating document, and wherein said step of generating said machine readable data string comprises the substep of converting said k – byte data string into bar code print data.

109. A method for creating a self-authenticating document having critical document data, said critical document data including machine-readable data printed on said self-authenticating document, said method comprising the steps of:

creating a first digital signature by signing said critical document data with a digital signature algorithm;

creating a second digital signature by signing said critical document data and a personal identification number (PIN) with said digital signature algorithm;

retrieving a public key certificate including an authentic public key for validating said first and second digital signatures;

determining whether said second digital signature is to be affixed to said self-authenticating document;

determining whether said first digital signature is to be affixed to said self-authenticating document;

affixing said public key certificate and at least one of said first digital signature and said second digital signature to said self-authenticating document in machine-readable code, based on the results of the second digital signature and first digital signature determining steps.

110. The method of claim 109, wherein said critical document data includes ASCII text from said self-authenticating document, and further comprising the step of:

storing said ASCII text in a machine-readable format on said self-authenticating document prior to said first digital signature creating step.

111. The method of claim 109, further comprising the steps of:

selecting a group of shared parameters corresponding to said digital signature algorithm for implementing said at least one of said first and second digital signatures;

generating a public key and a private key using said shared parameters;

certifying said public key via a certificate authority,

wherein said selecting, generating and certifying steps are carried out prior to said first digital signature creation step.

112. The method of claim 109, said step of creating said first digital signature includes the substeps of:

generating a public key and a private key using said digital signature algorithm;

assembling said critical document data said self-authenticating document; and,

applying said private key generated by said digital signature algorithm to said critical document data to create said first digital signature.

113. The method of claim 112, said step of creating said second digital signature includes the substeps of:

generating said personal identification number (PIN);

appending said personal identification number (PIN) to said critical document data to create an authenticatable data string; and,

applying said private key generated by said digital signature algorithm to said authenticatable data string to create said second digital signature.

114. The method of claim 109, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

115. The method of claim 109, wherein if it is determined that said first digital signature is to be affixed to said self-authenticating document, said step of affixing said first digital signature to said self-authenticating document includes the substeps of:

assembling a k – byte data string, wherein k includes the number of bytes in said critical document data; and,

generating a machine-readable data string from said k – byte data string.

116. The method of claim 109, wherein if it is determined that said second digital signature is to be affixed to said self-authenticating document, said step of affixing said second digital signature to said self-authenticating document includes the substeps of:

assembling a k – byte data string, wherein k includes the number of bytes in said authenticatable data string; and,

generating a machine-readable data string from said k – byte data string.

117. The method of claim 109, wherein if it is determined that said first and said second digital signatures are to be affixed to said self-authenticating document, said step of affixing said first and second digital signatures to said self-authenticating document includes the substeps of:

assembling a k – byte data string, wherein k includes the number of bytes in said critical document data and said authenticatable data string; and,

generating a machine-readable data string from said k – byte data string.

118. The method of claim 117, further comprising the step of calculating the total amount of bytes of data, k , in said critical document data and said authenticatable data string, prior to said k – byte data string assembling step.

119. A method of authenticating a self-authenticating document, comprising the steps of:

processing machine-readable data on said self-authenticating document to obtain digital signature data and a public key certificate;

processing said public key certificate to obtain public key certificate data including an authentic public key;

assembling critical document data from said self-authenticating document, wherein said critical document data includes at least magnetic ink character recognition (MICR) data printed on said self-authenticating document;

determining whether an authentic personal identification number (PIN) is available for appending to said critical document data;

wherein, if said authentic PIN is available;

appending said authentic PIN to said critical document data to create an authenticatable data string; and,

applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

120. The authenticating method of claim 119, wherein said self-authenticating document is a personal check, and wherein said critical document data includes ASCII text printed on said personal check.

121. The authenticating method of claim 119, further comprising the steps of:

determining whether a first digital signature is present in said digital signature data, if it is determined that said authentic personal identification number (PIN) is not available;

applying said authentic public key to said digital signature data to validate said critical document data, wherein said self-authenticating document is authenticated if said critical document data is validated.

122. The authenticating method of claim 121, wherein if it is determined that said authentic PIN is not available and that said first digital signature is not present in said digital signature data, further comprising the steps of:

determining whether a second digital signature is present in said digital signature data, and, if said second digital signature is present;

generating a plurality of PINs;

appending each of said plurality of PINs to said critical document data to create a plurality of verifiable data strings; and,

applying said authentic public key to said second digital signature in order to validate one of said verifiable data strings as said authenticatable data string and to authenticate said self-authenticating document.

123. The authenticating method of claim 122, wherein said step of generating PINs is carried out in a document reading system executing a PIN-generating algorithm.

124. The authenticating method of claim 121, wherein said machine-readable data is bar-code data, said machine-readable data processing step including the substeps of:

retrieving said bar code data from said self-authenticating document; and,

parsing data fields in said bar code data to obtain at least said public key certificate, said digital signature data, and k, where k, is the total number of bytes in said bar code data.

125. The authenticating method of claim 121, wherein said public key certificate data processing step includes the substeps of:

validating said public key certificate with a third-party public key; and,

parsing said public key certificate to obtain said authentic public key;

126. The authenticating method of claim 125, wherein said public key certificate includes a third-party digital signature, and wherein said public key certificate validating step further comprises the substep of applying said third-party public key to said third-party digital signature.

127. The authenticating method of claim 125, wherein said third party is a certificate authority.

128. The authenticating method of claim 125, wherein said public key certificate is comprised of m bytes, and wherein said public key certificate parsing substep includes the further substeps of:

retrieving at least a first byte, c_1, of said m bytes from said public key certificate, wherein said at least a first byte c_1 is a binary representation of said number of bytes m in said public key certificate;

determining whether said binary representation of said number of bytes m in said at least a first byte c_1, is greater than the number of bytes of data in said digital signature data, n;

retrieving the remainder of said m bytes, if said determining step determines that said at least a first byte c_1 is greater than the number of bytes of data in said digital signature data, n; and,

applying said authentic public key to said digital signature data in order to verify said at least one of said first and second digital signatures.

129. The authenticating method of claim 128, wherein said public key certificate parsing substep includes the further substeps of:

retrieving public key validity date data from said public key certificate;

determining if said public key validity date data is within an accepted date range; and,

validating said public key certificate with said public key validity date data, if said public key validity date data is within said accepted date range.

130. The authenticating method of claim 129, wherein said public key certificate parsing substep includes the further substep of:

issuing an alert if said public key validity date data is not within an accepted date range.

131. The authenticating method of claim 130, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by checking guidelines issued by said third party.

132. The authenticating method of claim 130, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by consulting a public key certificate database.

133. The authenticating method of claim 121, further comprising the step of :

presenting said self-authenticating document by an owner of said self-authenticating document to a commercial entity for authentication, wherein said presenting step is carried out prior to said machine-readable data processing step.

134. The authenticating method of claim 133, wherein said authentic PIN-determining step further includes the substep of:

determining whether an owner of said self-authenticating document is available to input said authentic PIN, wherein said PIN-availability step determines that said authentic PIN is not available if said owner of said self-authenticating document is not available.

135. A system for reading a self-authenticating document having machine-readable data including critical document data, digital signature data and a public key certificate, the system comprising:

personal identification means for receiving a personal identification number (PIN) from a presenter of said self-authenticating document; and,

image scanning and processing means for reading said self-authenticating document and retrieving said machine-readable data from said self-authenticating document, and for assembling an authenticatable data string from said critical document data and said received PIN;

parsing means for parsing said machine readable data to obtain said digital signature data and said public key certificate; and,

validating means for certifying said public key certificate to obtain an authentic public key, and for applying said authentic public key to said digital signature data for validating said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

136. The system of claim 135, wherein said machine-readable critical document data includes data stored in a first and second format on said self-authenticating document, and wherein said image scanning and processing means comprises:

a first machine-readable data reading system for reading said critical document data stored in a first format from said self-authenticating document; and,

a second machine-readable data reading system for reading said critical document data stored in a second format from said self-authenticating document.

137. The system of claim 136, wherein said first format is magnetic ink character recognition (MICR) code, and said second format is bar code, and wherein said first machine-readable data reading system reading system is a MICR reader, and said first machine-readable data reading system reading system is a bar code reader.

138. The system of claim 135, wherein said machine-readable critical document data is stored in a bar code format on said self-authenticating document, and wherein said image scanning and processing means includes a bar code reading system for reading said bar code format to retrieve said critical document data.

139. The system of claim 135, wherein said validating means comprises:

a certification validation subsystem for validating said public key certificate with a third party public key and for obtaining said authentic public key; and,

a digital signature validation subsystem for validating said digital signature data with said authentic public key.

140. A system for reading a self-authenticating document, said self-authenticating document having machine-readable data including first critical document data stored on a magnetic ink character recognition (MICR) line, and first and second digital signatures, and a public key certificate stored on a bar code line, the system comprising:

a personal identification subsystem for receiving a personal identification number (PIN) from a presenter of said self-authenticating document; and,

an image scanner and processor system for reading said self-authenticating document and retrieving said machine readable data from said self-authenticating document, and for assembling an authenticatable data string from said first critical document data and said received PIN, said image scanner and processor including:

a magnetic ink character recognition (MICR) reader subsystem for retrieving said first critical document data from said MICR line;

a bar code reader subsystem for retrieving said first and second digital signatures and said public key certificate stored on a bar code line;

a parsing subsystem for parsing said bar code to obtain said first and second digital signatures and said public key certificate; and,

a validating subsystem for certifying said public key certificate to obtain an authentic public key and for applying said authentic public key to at least said second digital signature for validating said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

141. The system of claim 140, wherein said machine-readable data further includes second critical document data stored in said bar code line, wherein said bar code reader subsystem further retrieves said second critical document data stored in said bar code line, and wherein said authenticatable data string assembled by said image scanner and processor subsystem includes said second critical document data.

142. The system of claim 141, wherein said second critical document data comprises ASCII text from said self-authenticating document.

143. The system of claim 142, wherein said ASCII text is the account name and address printed on said self-authenticating document.

144. The system of claim 140, wherein said validating means further applies said authentic public key to said first digital signature to validate said critical document data when no PIN is received, and wherein said self-authenticating document is authenticated if said critical document data is validated.

X. EVIDENCE APPENDIX

PART A **(FROM APPELLANTS' RESPONSE TO FINAL OFFICE ACTION INCLUDING NOTICE OF APPEAL, DATED SEPTEMBER 21, 2005):**

The Examiner continues to object to the claimed limitation "critical document data" as a term with relative meaning and thus possible of creating ambiguity. The Examiner's objection is erroneous for at least the following reasons.

It is well established that a patentee is his own lexicographer. *See, e.g., Universal Oil*, 137 F.2d 3, 6 (7th Cir. 1943), aff'd, 322 U.S. 471 (1944). Should the definition ascribed by the patentee to the term or terms used in the claim differ from the standard definition, the differing definition must be clearly set forth in the specification. *Beachcombers Int'l, Inc. v. WildeWood Creative Prods., Inc.*, 31 F.3d 1154, 1158, 31 USPQ2d 1653, 1656 (Fed. Cir. 1994) ("As we have repeatedly said, a patentee can be his own lexicographer provided the patentee's definition, to the extent it differs from the conventional definition, is clearly set forth in the specification.")

The Examiner bases his objection in large part on a subtitle found at page 15, lines 15-19, stating that the Applicants have defined "*'critical document data' as [a] 'personal value document having digital signature.'*" (Final Office Action, p. 2). The Examiner further contends that "*it is not clear if 'critical document data' have digital signatures or not*", and that "*one of ordinary skill in the art would not define 'critical document data' necessary [sic] having an embedded digital signature....*" (*Id. at* p. 3) However, a careful review of the ***entire*** specification, and particularly that encompassed by this subtitle, places it into context and reveals that the Examiner misinterprets the meaning of the subtitle as well as the meaning of "critical document data." More specifically, the subtitle, *in toto,* reads "A. Personal Value Document Having Digital Signature 1 (Critical Document Data), Digital Signature 2 (Critical Document Data and PIN) and Public Key Certificate." A thorough review of the applicable sections reveals that the embodiment of the invention disclosed therein is drawn to a Personal Value Document having: a first digital signature (digital signature 1) that is applied against the "critical document data;" a second digital signature (digital signature 2) that is applied against both the "critical document data" and a PIN (wherein the "critical document data" and the PIN are an "authenticatable data string"); and a public key certificate. (*09/707,433 Application,* pp. 15-18). Thus, the Examiner's contention that "critical document data" is a "personal value document having digital signature" is erroneous.

Furthermore, as previously stated in the May 16th Response, Applicants have provided a clear meaning to the term "critical document data" throughout the subject application (*see, e.g., 09/707,433 Application,* pp. 16-17). In particular, the application sets forth the following:

> *1. Critical Document Data*
>
> *In accordance with the preferred embodiment of the present invention, MICR code line 90 is designated as critical document data (FIG. 5). It is this critical document data that is targeted for enhanced security. (It will be appreciated that as there may be other data printed on a personal check 45 that are known at the time of printing, such as account name and address 92, which may are also be designated as part of that critical document data, and the scope of the present invention includes such data).*
>
> *In one aspect of a preferred embodiment of this invention, the entire preprinted MICR code line 90, including the special symbols 91 and 93 that identify particular MICR fields, is designated "critical document data"....*
>
> *Optionally, ASCII text strings (e.g., those identifying the account holder's name and address 92 in a personal value document) can also be designated critical document data....*
>
> *In accordance with another aspect of the preferred embodiment of the present invention, if such ASCII or other data is designated critical document data, it will need to be stored in machine-readable form on personal check 45 in a manner described in more detail in the forthcoming paragraphs. However, when the critical document data is simply the data that is stored in the MICR code line, there is no need to redundantly store this information in an alternate machine-readable format, as MICR characters are already machine-readable.*

(*Id. at* pp. 16-17, lines 5-34; 4-10). That the limitation "critical document data" may have alternate embodiments does not make it ambiguous.

In view of the foregoing, the Examiner's objection with regard to the claimed limitation "critical document data" as a term with relative meaning and thus possible of creating ambiguity cannot stand.

PART B (THE ORIGINAL TEXT OF PAGES 40-42 OF THE PENDING APPLICATION THAT IS THE SUBJECT OF THIS APPEAL):

Reference Number: PM021

4. If digital signature 1 validates (step 217), then the check is authenticated (step 210) because successful validation indicates that:

- the critical document data has not been altered or tampered with in any way since the bar code was produced.

The above steps would also be carried out in an alternate embodiment of the present invention, i.e., in the case where a customer presents a bank check or business check for deposit or cashing.

Finally, as digital signature 2 is preferred in the cases where only one digital signature is going to be printed on a personal value document (for the reasons set forth above), check reading system 100 might be programmed to check for digital signature 2 prior to checking for digital signature 1. Though it is preferred in those cases where the PIN or customer is unavailable to verify personal checks by first checking for the presence of digital signature 1, if only digital signature 2 were present on the check, check reading system 100 might first execute the PIN-generating algorithm or similar method until the personal check verifies.

1. *Parsing the bar code data string*

As set forth above, the bar code data on the value document is parsed by the payment system to find *k* (the total length bar code data string), *m* (the total length of the certificate), *l* (the length of the critical data field byte), digital signature 1 (if present) and digital signature 2 (if present).

The bar code string may be read from a 200 or 240 dot per inch gray scale image of the bar code, or it can be scanned using many different laser bar code scanners currently available. In either case, a string of bytes is retrieved from the bar code. Referring to FIG. 10, in order to parse the bar code data string into its component data fields, the following steps in a preferred method 203 are effected:

Reference Number: PM021

1. k, the binary representation the total number of bytes in the bar code is retrieve from the first two bytes of the bar code at step 301. All integers preferably are stored with the most significant bits on the left. Thus, for example, if b_1, b_2 are one byte integers stored as the first two bytes in the bar code data string, k is reconstructed as: $k = b_1 \cdot 2^8 + b_2$

2. The third byte is then retrieved from bar code data string at step 302. This byte is (a binary representation of) m, the total length of the certificate. Bytes 3 through $m+2$ are thus the printer certificate.

3. Byte $m+3$ is retrieved at step 303. This is l, the length of the critical data field string.

4. If $l=0$ (step 304), a critical data field string is not part of the bar code security data string and the process continues on to step 306; if $l \geq 1$, bytes $m+4$ through $m+l+3$ are the critical data string, and are retrieved at step 305.

5. As digital signature 2 comprises 42 bytes (21 bytes for r_2 and s_2 each) bytes $m+l+4$ through $m+l+45$ are then retrieved at step 306. If $b_{m+l+4}...b_{m+l+45}$ are the 1 byte integers which store digital signature 2, then

$$r_2 = \sum_{i=1}^{21} 2^{8(21-i)} b_{m+l+3+i} \text{ and,}$$

$$s_2 = \sum_{i=1}^{21} 2^{8(21-1)} b_{m+l+24+i}$$

Where digital signature 2 is (r_2, s_2).

Reference Number: PM021

6. If $k = 45 + m + l$ (step 307), then the process stops (step 308), as all fields have been extracted from the bar code. Otherwise, the barcode parsing proceeds to step 309.

7. At step 309, the sixth data field 66 (including digital signature 1), if present, is then extracted. As digital signature 1 also comprises 42 bytes (21 bytes for r_1 and s_1 each), k should be $k = 45 + m + l + 42$ or $87 + m + l$ (step 309). If $k \neq 87 + m + l$, then report an error and stop (step 310). Otherwise, digital signature 1 is extracted from bytes $b_{m+l+46}...b_{m+l+87}$ (step 311). Again interpreting each byte as a binary integer with most significant bit on the left, reconstruct (r_1, s_1) as

$$r_1 = \sum_{i=1}^{21} 2^{8(21-i)} b_{m+l+45+i}, \text{ and,}$$

$$s_1 = \sum_{i=1}^{21} 2^{8(21-i)} b_{m+l+66+i}.$$

All data fields should now be parsed from the bar code string and the process completed (step 312).

3. *Validating a Public Key Certificate*

Once the bar code string is parsed by parsing module 120, an attempt to validate public key certificate is made in validation module 130. As shown in FIG. 11, a preferred method 202 for validating an m-byte certificate includes the following steps:

1. Let $c_1...c_m$ represent the bytes in the certificate. According to the preferred embodiment, the first byte of the certificate, c_1, a binary representation of m, is retrieved at 401. As with digital signatures 1 and 2, in a preferred embodiment of the present invention, if $m \leq 42$ (step 402), the certificate is not valid and the process stops (step 403).